IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Hardjono Application No.: 09/607007 Filed: 06/29/2000 Title: System, Device and Method for Controlling Access in a Multicast Communication Network Attorney Docket No.: 2204/A46 120-147 Nortel: 12085BA	Group Art Unit: 2143 Examiner: Choudhury

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Sir:

Please enter this Reply Brief.

I. Real Party in Interest

The real party in interest is Nortel Networks, Limited.

II. Related Appeals and Interferences

Appellants are not aware of any related appeals or interferences.

III. Status of the Claims

Claims 1-8, 10-16, 18-25, 27-28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, and 131-145 are pending in this application. Claims 9, 17, 26, 29-30, 46, 62, 69, 76, 88, 106-107, 129-130, and 145-152 are cancelled. All of the pending claims are rejected. The precise status of all claims is shown in Appendix A. The rejections of independent claims 1, 16, 28, 40, 61, 68, 75, 87, 99 and 122 are the subject of this appeal.

IV. Status of Amendments

All submitted amendments have been entered and considered by the Office. A Notice of Appeal was filed on June 23, 2008.

V. Summary of Claimed Subject Matter

The presently claimed invention concerns a technique by which the authentication of a host device by a key server can be **verified** by a designated device. In particular, **after authenticating the host device**, the key server provides the host device with an access token that can be presented to the

designated device **to prove to the designated device that the host has been properly authenticated by the key server**. The access token includes a host identifier which identifies the host, a token identifier which identifies the token, and a group identifier which identifies the multicast group for which the host has been authenticated. Further, the token identifier is used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

The limitations recited in the independent claims are supported in the specification and drawing as indicated below in bold type. Additional support may exist.

1. (previously presented) A communication system comprising:

a plurality of multicast devices forming a shared multicast distribution tree **(Figure 1)**;

a host device **(host H1 112, figure 1)**;

a key server **(key server 118, figure 1)**; and

a designated device **(designated router DR1 110, figure 1)**, separate from the key server, through which the host device requests access to the shared tree associated with a group, wherein:

the host device obtains access information from the key server for the host device to enable the host device to request access to the shared tree associated with the group **("Obtain access information for joining a multicast group." step 504, FIG. 5)**, the access information including authentication information

unique to the host device/group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4)**;

the designated device obtains the access information associated with the host device/group pair from the key server for enabling the host device to access the shared tree **("Retrieve access information." Step 706, FIG. 7)**;

the host device sends an access control message to the designated device to join the shared tree **("Send the join request to the DR." Step 514, FIG. 5)**; and

the designated device uses the access information to authenticate the host device before adding the host device to the shared tree **("Authenticate the join request using the access information." Step 614, FIG. 6; See also Step 714, FIG. 7)**, including using the token identifier to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

16. (previously presented) A method performed at a key server comprising:

authenticating a host device for entry into a multicast group **("Authenticate the host." Step 404, FIG. 4)**;

generating access information by the key server for the host device to join the multicast group, the access information including authentication information unique to the host device/ multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting**

multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4);

sending the access information to the host device **("Forward the group key and the access information to the host." Step 408, FIG. 4)**; and

sending the access information to a separate designated device through which host device gains access to a shared multicast distribution tree **("Forward certain access information to the DR." Step 410, FIG. 4)**, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

28. (previously presented) A method performed at a host device comprising:

obtaining access information from a key server for joining a multicast group **("Obtain access information for joining a multicast group." step 504, FIG. 5)**, the access information including authentication information unique to the host device/ group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4)**;

generating an access control message for joining the multicast group using the access information **("Generate a join request using the access information." Step 512, FIG. 5)**; and

sending the access control message to a designated device separate from the key server for enabling the host device to join the multicast group **("Send the join request to the DR." Step 514, FIG. 5)**, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

40. (previously presented) A method performed at a designated device that controls access to a shared multicast tree comprising:

receiving an access control message from a host device **("Receive a join request from the host." Step 604, FIG. 6 and step 704, FIG. 7)**;

determining whether the host device is authorized to request access to a shared multicast distribution tree associated with a group based upon access information for the host device **("Retrieve access information." Step 706, FIG. 7; "Check expiration date to determine whether or not the access token has expired." Step 710, FIG. 7; "Authenticate the join request using the access information." Step 714, FIG. 7)**, the access information including authentication information unique to the host device/group pair and being received by the designated device from a separate key server, the authentication

information including a host identifier, an access token comprising a token identifier and an authentication key for authenticating the host with the designated device, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4)**; and

joining the shared tree on behalf of the host device if the host device is determined to be authorized to request access to the shared tree **("Forward a PIM join request upstream toward the RP and join the shared tree on behalf of the host." Step 720, FIG. 7)**.

61. (previously presented) An apparatus comprising:

authenticating logic operably coupled to authenticate a host device for entry into a multicast group **("Authenticate the host." Step 404, FIG. 4)**;

access logic operably coupled to generate access information for the host device, the access information including authentication information unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4)**; and

distribution logic operably coupled to distribute the access information both to the host device **("Forward the group key and the access information to the host." Step 408, FIG. 4)** and to a separate designated device **("Forward**

certain access information to the DR." Step 410, FIG. 4) for enabling the host device to access a shared multicast distribution tree through the designated device, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

68. (previously presented) A computer program for controlling a key server in a computer system, the computer program comprising:

authenticating logic programmed to authenticate a host device for entry into a multicast group **("Authenticate the host." Step 404, FIG. 4)**;

access logic programmed to generate access information for the host device the access information including authentication information unique of the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast**

data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4); and

distribution logic programmed to distribute the access information to the host device **("Forward the group key and the access information to the host." Step 408, FIG. 4)** and to a separate designated device **("Forward certain access information to the DR." Step 410, FIG. 4)** for enabling the host device to access a shared multicast distribution tree through the designated device, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

75. (previously presented) An apparatus comprising:

receiving logic operably coupled to receive, from an access information server, access information **("Obtain access information for joining a multicast group." step 504, FIG. 5)**, the access information enabling the host device to join a multicast group the access information being unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4)**; and

access logic operably coupled to generate an access control message for joining the multicast group using the access information **("Generate a join request using the access information." Step 512, FIG. 5)** and to send the

access control message to a designated device separate from the access information server **("Send the join request to the DR." Step 514, FIG. 5)** and coupling the host device to the multicast group, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

87. (previously presented) A computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive access information for joining a multicast group from an access information server **("Obtain access information for joining a multicast group." step 504, FIG. 5)**, the access information including authentication information unique to a host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the**

multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4); and

access logic programmed to generate an access control message for joining the multicast group using the access information **("Generate a join request using the access information." Step 512, FIG. 5)** and to send the access control message to a designated device separate from the access information server **("Send the join request to the DR." Step 514, FIG. 5)** and coupling the host device to the multicast group, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("When the DR receives a join request from the host including a token identifier, the DR uses the token identifier to obtain access information for the host/group pair from its access information database. The access information typically includes, among other things, the group identifier and authentication key." Page 11, lines 104)**.

99. (previously presented) An apparatus comprising:

receiving logic operably coupled to receive an access control message from a host device **("Receive a join request from the host." Step 604, FIG. 6 and step 704, FIG. 7)**, the access control message for permitting the host device to gain access to a multicast group, the access control message including authentication information unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4)**;

access logic operably coupled to determine whether the host device is authorized to access a shared multicast distribution tree based upon access

information for the host device stored at the apparatus, the stored access information including authentication information unique to the host device/multicast group pair and being received from a separate key server, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("Retrieve access information." Step 706, FIG. 7; "Check expiration date to determine whether or not the access token has expired." Step 710, FIG. 7; "Authenticate the join request using the access information." Step 714, FIG. 7)**; and

joining logic operably coupled to join the shared tree on behalf of the host device if the access logic determines that the host device is authorized to access the shared tree **("Forward a PIM join request upstream toward the RP and join the shared tree on behalf of the host." Step 720, FIG. 7)**.

122. (previously presented) A computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an access control message from a host device to enable the host device to join a multicast group **("Receive a join request from the host." Step 604, FIG. 6 and step 704, FIG. 7)**, the access control information including authentication information unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device **("FIG. 2 shows the relevant**

fields of an exemplary GKM message 200 for distributing the access information to the host. The GKM message 200 includes, among other things, a group key 202 and an access token 204. The group key 202 is an encryption key that is used by the multicast source for encrypting multicast data and by the multicast clients (hosts) for decrypting multicast data. The access token 204 includes access information for a particular host to access a particular multicast group. The GKM message 200 is sent by key server 118 to the host over a secure communication channel." Page 8, lines 18-25; "FIG. 3 shows the fields of an exemplary access token 204. The access token 204 includes a group identifier 302, a host identifier 304, a token identifier 306, an authentication key 308, an expiration date 310, a server identifier 312, and a server public key 314." Page 8, lines 26-29; See also steps 404, 406, 408 and 410 in FIG. 4);

access logic programmed to determine whether the host device is authorized to access a shared multicast distribution tree based upon stored access information for the host device, the stored access information including authentication information unique to the host device/multicast group pair and being received from a separate key server, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device **("Retrieve access information." Step 706, FIG. 7; "Check expiration date to determine whether or not the access token has expired." Step 710, FIG. 7;**

"Authenticate the join request using the access information." Step 714, FIG. 7); and

joining logic programmed to join the shared tree on behalf of the host device if the access logic determines that the host device is authorized to access the shared tree **("Forward a PIM join request upstream toward the RP and join the shared tree on behalf of the host." Step 720, FIG. 7)**.

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1, 16, 28, 40, 61, 68, 75, 87, 99 and 122 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5,748,736 (Mittra) in view of US 6,088,451 (He) and further in view of US 5,682,478 (Watson).

VII. Argument

A. The cited combination fails to teach verification of authentication

1. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

The presently claimed invention concerns a technique by which the authentication of a host device by a key server can be **verified** by a designated

device. In particular, after authenticating the host device, the key server provides the host device with an access token that can be presented to the designated device **to prove to the designated device that the host has been properly authenticated by the key server**.

With regard to each of the independent claims the examiner stresses that Mittra discloses separate key distribution centers which could be used for authentication within the tree architecture. The examiner specifically states at page 3 of the Office Action that Mittra's "key distribution centers" are equivalent to the "key server" recited in the claims. However, since the examiner also cites Mittra's "key distribution centers" in the section associated with the "designated device separate from the key server," it is apparent that the examiner believes that Mittra's key distribution centers are also equivalent to the designated devices (which are described as routers in the detailed description). These assertions illustrate a misunderstanding of the meaning of the claim limitations. What is recited is not a network in which authentication of a host might be performed by either a key server or a designated device. Rather, the key server authenticates the host and the designated device (router) **verifies** that the key server has authenticated the host before providing service. For example, claim 16 recites "A method **performed at a key server** comprising: **authenticating a host device** for entry into a multicast group." (emphasis added) Note that in the first element of the body of the claim the host is already authenticated by the key server. The claim subsequently recites "sending the access information to a separate designated device through which host device gains access to a shared multicast

distribution tree, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) Since the host has already been authenticated by the key server, the designated device is not simply an alternative authentication device. Indeed, the designated device is not authenticating the host at all, but is verifying prior authentication of the host by the key server. In view of the above, claim 16 distinguishes the cited combination of references even if the teachings of those references as characterized by the examiner are assumed to be accurate.

In order to provide a complete explanation of how the claims distinguish the cited combination, the corresponding limitations in the other independent claims are quoted below. For example, claim 1 recites "the designated device uses the access information to authenticate the host device before adding the host device to the shared tree, including using the token identifier to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) Similarly, claim 28 recites "sending the access control message to a designated device separate from the key server for enabling the host device to join the multicast group, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) Claim 40 recites "the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device.**" (emphasis added) Claim 61 recites

"the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device.**" (emphasis added) Claim 68 recites "the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device.**" (emphasis added) Claim 75 recites "the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) Claim 87 recites "the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) Claim 99 recites "the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) Claim 122 recites "the token identifier being used by the designated device to obtain a group identifier and authentication key from memory **in order to verify authentication of the host device**." (emphasis added) The cited references fail to show, and the examiner has failed to argue, the limitations emphasized above.

2. In response to the argument above, the Examiner now asserts[1] that Mittra's key distribution center (KDC) is equivalent to the claimed key server, and Mittra's group security controller (GSC) is equivalent to the claimed designated device that verifies that the key server has authenticated the host. This

[1] Examiner's Answer at page 19

novel reasoning is contradicted by both the Final Office Action[2] and Mittra. Further, the reasoning illustrates a failure to recognize the distinction between "authentication" and "verifying authentication," i.e., verification. Authentication establishes the validity of a claimed user or object. Verification establishes that authentication has already occurred. The rejection makes no distinction between authentication and verification, and consequently misinterprets Mittra. Neither the GSC nor the KDC of Mittra perform a verification function. As stated in Mittra at column 3, lines 36-42 regarding other protocols, "each of them relies on a per group key distribution center (KDC), also called the group controller (GC) in the Group Key Management Protocol (GKMP) proposed by Harney et al and called the management station (MS) by Tseung … [and] all members contact this KDC and upon successful **authentication** they receive the group key which they then use to decrypt multicast transmissions." (emphasis added) Note that the KDC performs authentication, not verification. Regarding the GSC, Mittra states at column 7, lines 32-35 that "the GSC (e.g., GSC 111 of FIG. 1) provides key management and thus effectively controls secure multicast group ("the group") membership … as far as the system is concerned all that is required to begin a secure multicast is that the GSC is started up … [and then] senders and receivers apply to join the group as described below." What is described "below" is that "once the GSC and the new member have **authenticated** each other and have agreed on a secret the GSC needs to provide the new member with information … ." (emphasis added) Note that the GSC performs authentication, not verification.

[2] At pp. 2-3 of the Final Office Action the only element from Mittra cited against the "designated device" is the KDC.

The new reason for rejection described in the Examiner's Answer is therefore flawed for the same reasons stated with regard to the previous rejection, and should be reversed.

B. The examiner improperly relies upon Official Notice

1. With regard to each of the independent claims the examiner asserts that the specific limitations associated with the access control information are inherent. At page 3 of the Office Action the examiner states "furthermore, it is inherent that authentication for each host device must be unique as claimed … because certificates apply public key cryptographic algorithms and public key algorithms require unique data for each user to be authenticated," and "during authentication, the access information must contain an id of some form to distinguish it; hence a member identifier must inherently be present." This assertion that features need not actually be shown in the references because they are "inherent" is equivalent to taking official notice because the Examiner attempts to extend the inherency beyond the cited reference. According to MPEP 2144.03(A), Official Notice without documentary evidence to support an examiner's conclusion should be rare when an application is **under final rejection** or action under 37 CFR 1.113. Appellant therefore challenges the propriety of the official notice in the final rejection.

As noted by the court in *In re Ahlert*, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970), the notice of facts beyond the record which may be

taken by the examiner must be "capable of such instant and unquestionable demonstration as to defy dispute" (citing *In re Knapp Monarch Co*., 296 F.2d 230, 132 USPQ 6 (CCPA 1961)). See also *In re Grose*, 592 F.2d 1161, 1167-68, 201 USPQ 57, 63 (CCPA 1979) ("[W]hen the PTO seeks to rely upon a chemical theory, in establishing a prima facie case of obviousness, it must provide evidentiary support for the existence and meaning of that theory."); *In re Eynde,* 480 F.2d 1364, 1370, 178 USPQ 470, 474 (CCPA 1973) ("[W]e reject the notion that judicial or administrative notice may be taken of the state of the art. The facts constituting the state of the art are normally subject to the possibility of rational disagreement among reasonable men and are not amenable to the taking of such notice."). In accordance with MPEP 2144.03(C), Appellant challenges the Examiner to produce a reference teaching that authentication of a host by a key server inherently includes authentication information unique to the host device/multicast group pair, including an access token comprising a host identifier, a token identifier and an authentication key **for verifying host authentication to the designated device**. In other words, that information must not only be unique to the host device/multicast group pair, but must also **be usable by a third device to verify that authentication has occurred between the key server and host**.

2. In response to the argument above the Examiner asserts that Official Notice requirements are inapplicable because inherency was argued rather than official notice. With all due respect, the Examiner misunderstands the

argument. The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993). To establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999). Applicant submits that not only is the limitation NOT inherent in the reference, but the reasoning behind the inherency argument is an impermissible extension lacking support of extrinsic evidence, and furthermore is actually false. The following statement by the Examiner is the "inherency" argument:

> Furthermore, it is inherent that authentication for each host device must be unique as claimed.

These subsequent statements are Official Notice because they do not relate to the hole in the reference or any extrinsic evidence, i.e., they have been pulled out of thin air[3]:

> This is because certificates apply public key cryptographic algorithms and public key algorithms require unique data for each user to be authenticated. During authentication, the access

[3] Note also that the Examiner conflates authentication with encryption. When considered in context, e.g., delivering television signals over secure multicast, authentication is used to assure that only subscribers are provided with access to the television signal, whereas encryption is used to secure the television signal against non-subscribers. The Examiner argues that authentication is a necessary part of encryption, but the functions are not necessarily related. For example, authenticating a non-subscriber would not reveal the encryption key to other non-subscribers.

> information must contain an id of some form to distinguish it.

Appellant submits that not only is the reasoning above an unsupported Official Notice, but it is also technically false. Public-key cryptography is a method for secret communication between two parties without requiring an initial authentication for secret key exchange. Public-key cryptography can be used in this manner because a user has a pair of keys: a public key and a private key. The private key is kept secret, while the public key may be widely distributed, i.e., no authentication required. Messages encrypted using the public key can only be decrypted with the corresponding private key. Security is provided because although the keys are related mathematically, the private key cannot be derived from the public key. Since the Examiner's statements above are not an inherency argument but rather an unsupported extension of an inherency argument, the rules of Official Notice should be applied. Further, because the statement is both unsupported and unsupportable, the rejection should be reversed.

VIII. Conclusion

Appellants submit that the rejections of the claims discussed above are improper for at least the reasons set forth. Appellants accordingly request that the rejections be withdrawn and the application put forward for allowance.

Respectfully submitted,

By: /Holmes W. Anderson/
Holmes W. Anderson
Reg. No. 37,272
Attorney for Assignee

Date: February 17, 2009

Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton MA 01720
(978) 264-4001

Appendix A - Claims

1. (previously presented) A communication system comprising:

a plurality of multicast devices forming a shared multicast distribution tree;

a host device;

a key server; and

a designated device, separate from the key server, through which the host device requests access to the shared tree associated with a group, wherein:

the host device obtains access information from the key server for the host device to enable the host device to request access to the shared tree associated with the group, the access information including authentication information unique to the host device/group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device;

the designated device obtains the access information associated with the host device/group pair from the key server for enabling the host device to access the shared tree;

the host device sends an access control message to the designated device to join the shared tree; and

the designated device uses the access information to authenticate the host device before adding the host device to the shared tree, including using the token identifier to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

2. (previously presented) The communication system of claim 1, wherein the key server includes logic for authenticating the host device and generating the access information for the host device to access the shared tree.

3. (original) The communication system of claim 2, wherein the key server provides the access information to the host device over a secure communication channel.

4. (original) The communication system of claim 2, wherein the key server provides the access information to the designated device using a unicast distribution mechanism.

5. (original) The communication system of claim 2, wherein the key server provides the access information to the designated device using a multicast distribution mechanism.

6. (original) The communication system of claim 2, wherein the key server provides the access information to the designated device using a broadcast distribution mechanism.

7. (original) The communication system of claim 2, wherein the designated device requests the access information from the key server upon receiving the access control message.

8. (original) The communication system of claim 2, wherein the key server provides the access information to the plurality of multicast devices forming the shared tree.

9. (cancelled)

10. (previously presented) The communication system of claim 1, wherein the access control message comprises the token identifier.

11. (original) The communication system of claim 10, wherein the access control message is an Internet Group Management Protocol (IGMP) join request including the token identifier.

12. (original) The communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device upon authenticating the host device.

13. (original) The communication system of claim 12, wherein the shared tree is a Protocol Independent Multicast (PIM) shared tree, and wherein the designated device

sends a PIM join request upstream toward a rendezvous point device in order to join the shared tree on behalf of the host device upon authenticating the host device.

14. (original) The communication system of claim 1, wherein the designated device forwards the access control message to a neighboring device upon failing to authenticate the host device using the access information.

15. (original) The communication system of claim 14, wherein the neighboring device obtains the access information and authenticates the host device using the access information.

16. (previously presented) A method performed at a key server comprising:

authenticating a host device for entry into a multicast group;

generating access information by the key server for the host device to join the multicast group, the access information including authentication information unique to the host device/ multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device;

sending the access information to the host device; and

sending the access information to a separate designated device through which host device gains access to a shared multicast distribution tree, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

17. (cancelled)

18. (previously presented) The method of claim 16, wherein the access information further comprises an expiration date for the access token.

19. (original) The method of claim 16, wherein the access information further comprises a public key.

20. (original) The method of claim 16, wherein sending the access information to the host device comprises:

sending a communication message including the access information to the host device over a secure communication channel.

21. (original) The- method of claim 20, wherein the communication message is a group key management communication message.

22. (original) The method of claim 16, wherein sending the access information to the designated device for the host device comprises:

sending a communication message including the access information to the designated device over a secure communication channel.

23. (original) The method of claim 22, wherein the communication message is a unicast communication message addressed to the designated device.

24. (original) The method of claim 22, wherein the communication message is a multicast communication message addressed to a multicast group of which the designated device is a member.

25. (original) The method of claim 22, wherein the communication message is a broadcast communication message.

26. (cancelled)

27. (previously presented) The method of claim 16, wherein the access token comprises:
a group identifier for identifying a multicast group;

a host identifier for identifying the host device;

an expiration date for the access token;

a server identifier for identifying a key server; and a public key for the key server.

28. (previously presented) A method performed at a host device comprising:

obtaining access information from a key server for joining a multicast group, the access information including authentication information unique to the host device/ group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device;

generating an access control message for joining the multicast group using the access information; and

sending the access control message to a designated device separate from the key server for enabling the host device to join the multicast group, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

29. (cancelled)

30. (cancelled)

31. (previously presented) The method of claim 28, further comprising:

generating authentication information using the access information; and sending the authentication information to the designated device.

32. (original) The method of claim 31, wherein generating the authentication information using the access information comprises generating a digital signature using the access information and a predetermined digital signature scheme.

33. (original) The method of claim32, wherein the predetermined digital signature scheme comprises a keyed hash function.

34. (previously presented) The method of claim 33, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using Message Digest 5 (HMAC-MD5).

35. (previously presented) The method of claim 33, wherein the keyed hash function comprises IP with Keyed-Hashing for Message Authentication using a Secure Hash Algorithm (HMAC-SHA-1).

36. (previously presented) The method of claim 29, wherein the access information further comprises an expiration date for the access token.

37. (original) The method of claim 36, wherein generating the access control message using the access information comprises:

including the token identifier in the access control message.

38. (original) The method of claim 37, wherein the access control message is an Internet Group Management Protocol (IGMP) join request message including the token identifier.

39. (original) The method of claim 28, further comprising:
establishing a security agreement with the designated device using the access information.

40. (previously presented) A method performed at a designated device that controls access to a shared multicast tree comprising:

receiving an access control message from a host device;

determining whether the host device is authorized to request access to a shared multicast distribution tree associated with a group based upon access information for the host device, the access information including authentication information unique to the host device/group pair and being received by the designated device from a separate key server, the authentication information including a host identifier, an access token comprising a token identifier and an authentication key for authenticating the host with

the designated device, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device; and

joining the shared tree on behalf of the host device if the host device is determined to be authorized to request access to the shared tree.

41. (original) The method of claim 40, further comprising:

obtaining the access information for the host device.

42. (original) The method of claim 41, wherein obtaining the access information for the host device comprises:

receiving the access information from an access information server prior to receiving the access control message from the host device.

43. (original) The method of claim 41, wherein obtaining the access information for the host device comprises:

requesting the access information from an access information server after receiving the access control message from the host device.

44. (original) The method of claim 40, wherein determining whether the host device is authorized to access the shared tree comprises:

maintaining an access information database;

searching the access information database for the access information for the host device;

failing to find the access information for the host device in the access information database; and

determining that the host device is not authorized to access the shared tree.

45. (original) The method of claim 40, wherein determining whether the host device is authorized to access the shared tree comprises:

maintaining an access information database;

searching the access information database for the access information for the host device;

failing to find the access information for the host device in the access information database; and

forwarding the access control message to a neighboring device.

46. (cancelled)

47. (original) The method of claim 40, wherein the access control message includes the token identifier.

48. (previously presented) The method of claim 40, wherein the access information further comprises an expiration date for the access token.

49. (previously presented) The method of claim 48, wherein determining whether the host device is authorized to access the shared tree comprises:

determining that the access token has expired based upon the expiration date for the access token; and

determining that the host device is not authorized to access the shared tree in response to expiration of the access token.

50. (previously presented) The method of claim 48, wherein determining whether the host device is authorized to access the shared tree comprises:

determining that the access token has expired based upon the expiration date for the access token; and

forwarding the access control message to a neighboring device.

51. (original) The method of claim 40, wherein determining whether the host device is authorized to access the shared tree comprises:

authenticating the host device using the access information and a predetermined authentication scheme; and

determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme.

52. (original) The method of claim 51, wherein authenticating the host device using the access information and the predetermined authentication scheme comprises:

receiving authentication information from the host device; and authenticating the host device based upon the access information and the authentication information received from the host device.

53. (original) The method of claim 52, wherein the authentication information comprises a digital signature, and wherein authenticating the host device based upon the access information and the authentication information received from the host device comprises:

verifying the digital signature using the access information and a predetermined digital signature scheme.

54. (original) The method of claim 53, wherein the predetermined digital signature scheme comprises a keyed hash function.

55. (previously presented) The method of claim 54, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using Message Digest 5 (HMAC-MD5).

56. (previously presented) The method of claim 54, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using a Secure Hash Algorithm (HMAC-SHA-1).

57. (original) The method of claim 51, wherein determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme comprises:
determining that authentication failed;

determining that the host device is not authorized to access the shared tree.

58.(original) The method of claim 57, further comprising:

forwarding the access control message to a neighboring device.

59. (original) The method of claim 51, wherein determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme comprises:

determining that authentication succeeded; and

determining that the host device is authorized to access the shared tree.

60. (original) The method of claim 40, further comprising:

establishing a security association with the host device using the access information upon determining that the host device is authorized to access the shared tree.

61. (previously presented) An apparatus comprising:

authenticating logic operably coupled to authenticate a host device for entry into a multicast group;

access logic operably coupled to generate access information for the host device, the access information including authentication information unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device; and

distribution logic operably coupled to distribute the access information both to the host device and to a separate designated device for enabling the host device to access a shared multicast distribution tree through the designated device, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

62. (cancelled)

63. (previously presented) The apparatus of claim 61 wherein the access token comprises: a group identifier for identifying a multicast group;

an expiration date for the access token;

a server identifier for identifying a key server; and a public key for a key server.

64. (original) The apparatus of claim 61, wherein the distribution logic comprises:

group key management logic operably coupled to send the access information to the host device.

65. (original) The apparatus of claim 61, wherein the distribution logic comprises: unicasting logic operably coupled to send the access information to the designated device using a unicast mechanism.

66. (original) The apparatus of claim 61, wherein the distribution logic comprises: multicasting logic operably coupled to send the access information to the designated device using a multicast mechanism.

67. (original) The apparatus of claim 61, wherein the distribution logic comprises: broadcasting logic operably coupled to send the access information to the designated device using a broadcast mechanism.

68. (previously presented) A computer program for controlling a key server in a computer system, the computer program comprising:

authenticating logic programmed to authenticate a host device for entry into a multicast group;

access logic programmed to generate access information for the host device the access information including authentication information unique of the host device/multicast group pair , the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device; and

distribution logic programmed to distribute the access information to the host device and to a separate designated device for enabling the host device to access a shared multicast distribution tree through the designated device, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

69. (cancelled)

70. (previously presented) The computer program of claim 68 wherein the access token comprises:

a group identifier for identifying a multicast group;

an expiration date for the access token;

a server identifier for identifying a key server; and a public key for a key server.

71. (original) The computer program of claim 68, wherein the distribution logic comprises:

group key management logic programmed to send the access information to the host device:

72. (original) The computer program of claim 68, wherein the distribution logic comprises:

unicasting logic programmed to send the access information to the designated device using a unicast mechanism.

73. (original) The computer program of claim 68, wherein the distribution logic comprises:

multicasting logic programmed to send the access information to the designated device using a multicast mechanism.

74. (original) The computer program of claim 68, wherein the distribution logic comprises:

broadcasting logic programmed to send the access information to the designated device using a broadcast mechanism.

75. (previously presented) An apparatus comprising:

receiving logic operably coupled to receive, from an access information server, access information, the access information enabling the host device to join a multicast group the access information being unique to the host device/multicast group pair , the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device; and

access logic operably coupled to generate an access control message for joining the multicast group using the access information and to send the access control message to a designated device separate from the access information server and coupling the host device to the multicast group, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

76. (cancelled)

77. (previously presented) The apparatus of claim 75, wherein the access logic is operably coupled to include the token identifier in the access control message.

78. (original) The apparatus of claim 75, wherein the access logic is operably coupled to generate authentication information using the access information and send the authentication information to the designated device.

79. (original) The apparatus of claim 78, wherein the access logic is operably coupled to generate the authentication information by generating a digital signature using the access information and a predetermined digital signature scheme.

80. (original) The apparatus of claim 79, wherein the predetermined digital signature scheme comprises a keyed hash function.

81. (previously presented)The apparatus of claim 80, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using Message Digest 5 (HMAC-MD5).

82. (previously presented) The apparatus of claim 80, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using a Secure Hash Algorithm (HMAC-SHA-1).

83. (previously presented) The apparatus of claim 76, wherein the access information further comprises an expiration date for the access token.

84. (previously presented) The apparatus of claim 75, wherein the access logic is operably coupled to include the token identifier in the access control message.

85. (original) The apparatus of claim 84, wherein the access control message is an Internet Group Management Protocol (IGMP) join request message including the token identifier.

86. (original) The apparatus of claim 75, wherein the access logic is operably coupled to establish a security agreement with the designated device using the access information.

87. (previously presented) A computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive access information for joining a multicast group from an access information server, the access information including authentication information unique to a host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device; and

access logic programmed to generate an access control message for joining the multicast group using the access information and to send the access control message to a designated device separate from the access information server and coupling the host device to the multicast group, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

88. (cancelled)

89. (previously presented) The computer program of claim 87, wherein the access logic is programmed to include the token identifier in the access control message.

90. (original) The computer program of claim 87, wherein the access logic is programmed to generate authentication information using the access information and send the authentication information to the designated device.

91. (original) The computer program of claim 90, wherein the access logic is programmed to generate the authentication information by generating a digital signature using the access information and a predetermined digital signature scheme.

92. (original) The computer program of claim 91, wherein the predetermined digital signature scheme comprises a keyed hash function.

93. (previously presented) The computer program of claim 92, wherein the keyed hash function comprises IPsec with Keyed-Hashing for Message Authentication using Message Digest 5 (HMAC-MD5).

94. (previously presented)The computer program of claim 92, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using a Secure Hash Algorithm (HMAC-SHA-1).

95. (previously presented) The computer program of claim 88, wherein the access information further comprises an expiration date for the access token.

96. (previously presented) The computer program of claim 88, wherein the access logic is programmed to include the token identifier in the access control message.

97. (original) The computer program of claim 96, wherein the access control message is an Internet Group Management Protocol (IGMP) join request message including the token identifier.

98. (original) The computer program of claim 87, wherein the access logic is programmed to establish a security agreement with the designated device using the access information.

99. (previously presented) An apparatus comprising:

receiving logic operably coupled to receive an access control message from a host device, the access control message for permitting the host device to gain access to a multicast group, the access control message including authentication information unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token identifier and an authentication key for authenticating the host with the designated device;

access logic operably coupled to determine whether the host device is authorized to access a shared multicast distribution tree based upon access information for the host device stored at the apparatus, the stored access information including authentication information unique to the host device/multicast group pair and being received from a separate key server, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device; and

joining logic operably coupled to join the shared tree on behalf of the host device if the access logic determines that the host device is authorized to access the shared tree.

100. (original) The apparatus of claim 99, wherein the access logic is operably coupled to obtain the access information for the host device from an access information server.

101. (original) The apparatus of claim 100, wherein the access logic is operably coupled to obtain the access information for the host device from the access information server prior to receiving the access control message from the host device.

102. (original) The apparatus of claim 100, wherein the access logic is operably coupled to obtain the access information for the host device from the access information server after receiving the access control message from the host device.

103. (original) The apparatus of claim 99, further comprising an access information database.

104. (original) The apparatus of claim 103, wherein the access logic is operably coupled to search the access information database for the access information for the host device and determine that the host device is not authorized to access the shared tree upon failing to find the access information for the host device in the access information database.

105. (original) The apparatus of claim 103, wherein the access logic is operably coupled to search the access information database for the access information for the host device and forward the access control message to a neighboring device upon failing to find the access information for the host device in the access information database.

106. (cancelled)

107. (cancelled)

108. (previously presented) The apparatus of claim 99, wherein the access information further comprises an expiration date for the access token.

109. (previously presented) The apparatus of claim 108, wherein the access logic is operably coupled to determine whether the host device is authorized to access the shared tree based upon the expiration date of the access token.

110. (previously presented) The apparatus of claim 109, wherein the access logic is operably coupled to determine that the host device is not authorized to access the shared tree upon determining that the access token has expired.

111. (previously presented) The apparatus of claim 109, wherein the access logic is operably coupled to forward the access control message to a neighboring device upon determining that the access token has expired based upon the expiration date for the access token.

112. (original) The apparatus of claim 99, wherein the access logic is operably coupled to authenticate the host device using the access information and a predetermined authentication scheme.

113. (original) The apparatus of claim 112, wherein the access logic is operably coupled to receive authentication information from the host device and authenticate the host device based upon the access information and the authentication information received from the host device.

114. (original) The apparatus of claim 113, wherein the authentication information comprises a digital signature, and wherein the access logic is operably coupled to verify the digital signature using the access information and a predetermined digital signature scheme.

115. (original) The apparatus of claim 114, wherein the predetermined digital signature scheme comprises a keyed hash function.

116. (previously presented) The apparatus of claim 115, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using Message Digest 5 (HMAC-MD5).

117. (previously presented) The apparatus of claim 115, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using a Secure Hash Algorithm (HMAC-SHA-1).

118. (original) The apparatus of claim 112, wherein the access logic is operably coupled to determine that the host device is not authorized to access the shared tree upon determining that the authentication failed.

119. (original) The apparatus of claim 118, wherein the access logic is operably coupled to forward the access control message to a neighboring device upon determining that the authentication failed.

120. (original) The apparatus of claim 112, wherein the access logic is operably coupled to determine that the host device is authorized to access the shared tree upon determining that the authentication succeeded.

121. (original) The apparatus of claim 99, wherein the access information is operably coupled to e(original) upon determining that the host device is authorized to access the shared tree.

122. (previously presented) A computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an access control message from a host device to enable the host device to join a multicast group, the access control information including authentication information unique to the host device/multicast group pair, the authentication information including an access token comprising a host identifier, a token

identifier and an authentication key for authenticating the host with the designated device;

access logic programmed to determine whether the host device is authorized to access a shared multicast distribution tree based upon stored access information for the host device, the stored access information including authentication information unique to the host device/multicast group pair and being received from a separate key server, the token identifier being used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device; and

joining logic programmed to join the shared tree on behalf of the host device if the access logic determines that the host device is authorized to access the shared tree.

123. (original) The computer program of claim 122, wherein the access logic is programmed to obtain the access information for the host device from an access information server.

124. (original) The computer program of claim 123, wherein the access logic is programmed to obtain the access information for the host device from the access information server prior to receiving the access control message from the host device.

125. (original) The computer program of claim 123, wherein the access logic is programmed to obtain the access information for the host device from the access information server after receiving the access control message from the host device.

126. (original) The .computer program of claim 122, further comprising an access information database.

127. (original) The computer program of claim 126, wherein the access logic is programmed to search the access information database for the access information for the host device and determine that the host device is not authorized to access the shared tree upon failing to find the access information for the host device in the access information database.

128. (original) The computer program of claim 126, wherein the access logic is programmed to search the access information database for the access information for the host device and forward the access control message to a neighboring device upon failing to find the access information for the host device in the access information database.

129. (cancelled)

130. (cancelled)

131. (previously presented) The computer program of claim 122, wherein the access information further comprises an expiration date for the access token.

132. (previously presented) The computer program of claim 131, wherein the access logic is programmed to determine whether the host device is authorized to access the shared tree based upon the expiration date for the access token.

133. (previously presented) The computer program of claim 132, wherein the access logic is programmed to determine that the host device is not authorized to access the shared tree upon determining that the access token has expired.

134. (previously presented) The computer program of claim 132, wherein the access logic is programmed to forward the access control message to a neighboring device upon determining that the access token has expired.

135. (original) The computer program of claim 122, wherein the access logic is programmed to authenticate the host device using the access information and a predetermined authentication scheme.

136. (original) The computer program of claim 135, wherein the access logic is programmed to receive authentication information from the host device and authenticate

the host device based upon the access information and the authentication information received from the host device.

137. (original) The computer program of claim 136, wherein the authentication information comprises a digital signature, and wherein the access logic is programmed to verify the digital signature using the access information and a predetermined digital signature scheme.

138. (original) The computer program of claim 137, wherein the predetermined digital signature scheme comprises a keyed hash function.

139. (previously presented) The computer program of claim 138, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using Message Digest 5 (HMAC-MD5).

140. (previously presented) The computer program of claim 138, wherein the keyed hash function comprises IPsec AH with Keyed-Hashing for Message Authentication using a Secure Hash Algorithm (HMAC-SHA-1).

141. (original) The computer program of claim 135, wherein the access logic is programmed to determine that the host device is not authorized to access the shared tree upon determining that the authentication failed.

142. (original) The computer program of claim 141, wherein the access logic is programmed to
forward the access control message to a neighboring device upon determining that the authentication failed.

143. (original) The computer program of claim 135, wherein the access logic is programmed to determine that the host device is authorized to access the shared tree upon determining that the authentication succeeded.

144. (original) The computer program of claim 122, wherein the access information is programmed to establish a security association with the host device using the access information upon determining that the host device is authorized to access the shared tree.

145. (cancelled)

146. (cancelled)

147. (cancelled)

148. (cancelled)

149. (cancelled)

150. (cancelled)

151. (cancelled)

152. (cancelled)

Appendix B - Evidence Submitted

None.

Appendix C - Related Proceedings

None.